

RECEIVED
CENTRAL FAX CENTER

APR 25 2006

Yee &
Associates, P.C.4100 Alpha Road
Suite 1100
Dallas, Texas 75244Main No. (972) 385-8777
Facsimile (972) 385-7766

Facsimile Cover Sheet

To: Commissioner for Patents for Examiner Longblt Chai Group Art Unit 2131	Facsimile No.: 571/273-8300
From: Jennifer Pilcher Legal Assistant to Wayne Bailey	No. of Pages Including Cover Sheet: 20
Message: Enclosed herewith: <ul style="list-style-type: none">• Transmittal of Appeal Brief; and• Appeal Brief.	
Re: Application No. 09/731,623 Attorney Docket No: AUS920000706US1	
Date: Tuesday, April 25, 2006	
Please contact us at (972) 385-8777 if you do not receive all pages indicated above or experience any difficulty in receiving this facsimile.	<i>This Facsimile is intended only for the use of the addressee and, if the addressee is a client or their agent, contains privileged and confidential information. If you are not the intended recipient of this facsimile, you have received this facsimile inadvertently and in error. Any review, dissemination, distribution, or copying is strictly prohibited. If you received this facsimile in error, please notify us by telephone and return the facsimile to us immediately.</i>

**PLEASE CONFIRM RECEIPT OF THIS TRANSMISSION BY
FAXING A CONFIRMATION TO 972-385-7766.**

RECEIVED
CENTRAL FAX CENTER

APR 25 2006

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Rinkevich et al.

Serial No.: 09/731,623

Filed: December 7, 2000

For: Aggregated Authenticated
Identity Apparatus for and Method
Therefor

§
§
§
§
§
§

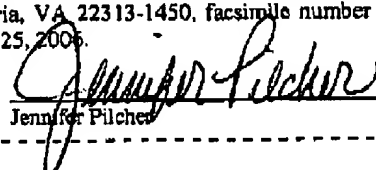
Group Art Unit: 2131

Examiner: Chal, Longbit

Attorney Docket No.: AUS920000706US1

35525

PATENT TRADEMARK OFFICE
CUSTOMER NUMBER

Certificate of Transmission Under 37 C.F.R. § 1.8(a)
I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (571) 273-8300
on April 25, 2006.
By: 
Jennifer Pilcher

TRANSMITTAL OF APPEAL BRIEF

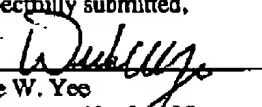
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:
ENCLOSED HEREWITH:

- Appeal Brief (37 C.F.R. 41.37)

A fee of \$500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

Respectfully submitted,


Duke W. Yee
Registration No. 36,285
YEE & ASSOCIATES, P.C.
P.O. Box 802333
Dallas, Texas 75380
(972) 385-8777
ATTORNEY FOR APPLICANTS

RECEIVED
CENTRAL FAX CENTER

APR 25 2006

Docket No. AUS920000706US1

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Rinkevich et al.

Serial No. 09/731,623

Filed: December 7, 2000

For: Aggregated Authenticated
Identity Apparatus for and Method
Therefor

§

§

§

§

§

§

§

§

Group Art Unit: 2131

Examiner: Chal, Longbit

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

35525

PATENT TRADEMARK OFFICE
CUSTOMER NUMBERCertificate of Transmittal Under 37 C.F.R. § 1.8(a)I hereby certify this correspondence is being transmitted via
facsimile to the Commissioner for Patents, P.O. Box 1450,
Alexandria, VA 22313-1450, facsimile number (571) 273-8300
on April 25, 2006.

By:

Jennifer Pilcher

APPEAL BRIEF (37 C.F.R. 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on February 28, 2006.

A fee of \$500.00 is required for filing an Appeal Brief. Please charge this fee to IBM Corporation Deposit Account No. 09-0447. No additional fees are believed to be necessary. If, however, any additional fees are required, I authorize the Commissioner to charge these fees which may be required to IBM Corporation Deposit Account No. 09-0447. No extension of time is believed to be necessary. If, however, an extension of time is required, the extension is requested, and I authorize the Commissioner to charge any fees for this extension to IBM Corporation Deposit Account No. 09-0447.

04/26/2006 TL0111 00000040 090447 09731623

01 FC:1402 500.00 DA

(Appeal Brief Page 1 of 18)
Rinkevich et al. - 09/731,623

REAL PARTY IN INTEREST

The real party in interest in this appeal is the following party: International Business Machines Corporation of Armonk, N.Y.

RELATED APPEALS AND INTERFERENCES

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no such appeals or interferences.

STATUS OF CLAIMS

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-24

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims canceled: none
2. Claims withdrawn from consideration but not canceled: none
3. Claims pending: 1-24
4. Claims allowed: none
5. Claims rejected: 1-24
6. Claims objected to: none

C. CLAIMS ON APPEAL

The claims on appeal are: 1-24

STATUS OF AMENDMENTS

A response to final office action was filed by Appellants on January 30, 2006, and was indicated by the Examiner as not being entered in an Advisory Action dated February 16, 2006.

SUMMARY OF CLAIMED SUBJECT MATTER**A. CLAIM 1 - INDEPENDENT**

Claim 1 is generally directed to a technique for managing authentication such that when a first security context is created in response to a first user authentication, a second security context is created in response to a second user authentication *which aggregates the two security contexts together*, thereby enabling finer granularity for each individual security context. Specifically, Claim 1 recites an authentication method, where a first security context is generated in response to a first user authentication. A second security context is generated in response to a second user authentication, where the second security context aggregates the first security context and a security context corresponding to an identify in the second user authentication (Specification page 10, line 16 – page 11, line 22; FIG 3, blocks 302, 304, 310 and 312).

B. CLAIM 9

Claim 9 is a program product claim corresponding to method Claim 1, and the summary of Claim 1 is applicable for Claim 9, and thus is hereby incorporated by reference.

C. CLAIM 17

Claim 17 is a system claim corresponding to method Claim 1, and the summary of Claim 1 is applicable for Claim 17, and thus is hereby incorporated by reference.

GROUND OF REJECTION TO BE REVIEWED ON APPEAL**A. GROUND OF REJECTION 1 (Claims 6, 14 and 22)**

Claims 6, 14 and 22 stand rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the enablement requirement.

B. GROUND OF REJECTION 2 (Claims 1-24)

Claims 1-24 stand rejected under 35 U.S.C. § 103 (a) as being unpatentable over Savill (Where can I find a Unix su like utility?) and in view of Wu (U.S. Patent Number 5,774,551), hereinafter referred to as Wu.

ARGUMENT

A. GROUND OF REJECTION 1 (Claims 6, 14 and 22)

A.1. Claims 6, 14 and 22

In rejecting Claim 6 (and Claims 14 and 22) under 35 U.S.C. § 112, first paragraph, the Examiner states that the claim limitation "by a user who issued the user logoff" is unclear, and thus not enabled. Appellants urge that specification support for Claim 6 is at Specification page 13, lines 2 -14 and lines 21-22, and depicted in Figure 3, blocks 314-320. There, if a user logout is received the current security context is destroyed and a reversion is made to use the (previously) saved security context if aggregation is enabled. This allows a given user to login using different security contexts (Specification page 2, lines 12-20; page 3, lines 8-20). Thus, when the reversion is made to use the (previous) saved security context, the user who issued the logoff from the second context is able to continue to use the first context that existed prior to the second context being created. It is thus urged that the Specification does describe the features recited in Claim 6, and thus Claim 6 is enabled by the Specification.

In an Advisory Action dated 2/16/06, the Examiner erroneously states that Claim 1 recites a 'first user' and a 'second user', and therefore the claimed feature of "reverting to said first security context in response to a user logoff, wherein said first security context is then used to access security protected resources by a user who issued the user logoff" is being interpreted as being "said first security context is then used to access security protected resources *by the second user*" (emphasis added by Appellants), and as such is not enabled. Applicants show error, in that contrary to the Examiner's assertion, Claim 1 recites "a first security *context*" and a "second security *context*" (and *not* a 'first user' and a 'second user', as alleged by the Examiner). As per the Specification, a single user can have different security contexts (Specification page 2, lines 14-20), the different security contexts being generated in response to different user authentications (Specification page 5, lines 5-6). The claimed authentication mechanism allows such a single user to selectively authenticate without necessarily giving up already established access, and as per the features of Claim 6, the user who issued the logoff from the second context is able to continue to use the first context that existed prior to the second context being created (Specification page 13, lines 2 -14 and lines 21-22, and depicted in Figure 3, blocks 314-320).

Therefore, the rejection of Claims 6, 14 and 22 under 35 U.S.C. § 112, first paragraph is shown to be in error, as the features recited in Claim 6 are in fact described in the specification, and thus are enabled.

B. GROUND OF REJECTION 2 (Claims 1-24)

B.1. Claims 1-5, 7-13, 15-21 and 23-24

With respect to Claim 1, Applicant's urge that Wu's stacking of authentication services is not done in response to a second user authentication, but rather is pre-existing and independent of any actual user authentication action. Importantly, Wu expressly teaches away from a second user authentication, or of performing any action in response to such (missing) second user authentication, by its teaching of a *unified, single user login*. See, for example, Wu's discussion at col. 3, lines 11-14, where it states:

"It is also desirable to provide a system and method where user is able to employ a single authentication token with any number multiple authentication services to obtain a unified login." (emphasis added by Applicants)

Because of this expressed desire by Wu to provide a *single authentication token* for accessing any number of multiple authentication services in order to obtain a unified (single) login, there would have been no reason or other motivation for Wu to perform any action in response to receiving a *second* user authentication (in addition to the first user authentication). Thus, there would have been no reason or other motivation to modify the teachings of the cited references to generate a second security context *in response to a second user authentication*, where this second security context is *an aggregate of* (i) said first security context and (ii) a security context *corresponding to an identity in said second user authentication*, as Wu abhors any type of such second user authentication. It is error to reconstruct the patentee's claimed invention from the prior art by using the patentee's claims as a "blueprint". When prior art references require selective combination to render obvious a subsequent invention, there must be some reason for the combination other than the hindsight obtained from the invention itself. *Interconnect*

Planning Corp. v. Feil, 774 F.2d 1132, 227 USPQ 543 (Fed. Cir. 1985). When an obviousness determination is based on multiple prior art references, there must be a showing of some "teaching, suggestion, or reason" to combine the references. "...absence of such suggestion to combine is dispositive in an obviousness determination". *Gambro Lundia AB v. Baxter Healthcare Corp.*, 110 F.3d 1573, 42 USPQ2d 1378 (Fed. Cir. 1997). Because of Wu's expressed desire to eliminate any need for a second user authentication – instead providing a unified login with a single user token – there would have been no motivation to one of ordinary skill in the art to modify the teachings of the cited references to generate a second security context (the second security context being an aggregate of (i) the first security context which was generated in response to a first user authentication, and (ii) a security context corresponding to an identity in the (missing) second security context) *in response to* a (missing) second user authentication).

In response to the above argument that "Wu expressly teaches away from a second user authentication", the Examiner states in an Advisory Action dated 2/16/2006 that this argument is without merit since the alleged limitation has not been recited in the claim. Applicants are reproducing herewith the identical language from Claim 1, with the relevant text highlighted to show that Claim 1 *does* in fact expressly recite a *second user authentication*:

Claim 1:

An authentication method comprising the steps of:

generating a first security context in response to a first user authentication;

generating a second security context in response to a second user authentication, wherein said second security context is an aggregate of said first security context and a security context corresponding to an identity in said **second user authentication**.

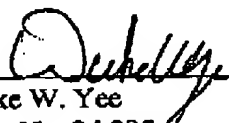
It is therefore urged that the missing claimed feature which Wu expressly teaches away from (a second user authentication) is expressly recited in Claim 1, and therefore the Examiner's reasoning in maintaining the final rejection of Claim 1 is shown to be in error.

B.2. Claims 6, 14 and 22

Further with respect to Claim 6 (and similarly for Claims 14 and 22), it is urged that a prima facie case of obviousness has not been properly established by the Examiner, and thus Claim 6 has been erroneously rejected¹. Claim 6 expressly recites "reverting to said first security context in response to a user logoff, wherein said first security context is then used to access security protected resources by a user who issued the user logoff". In rejecting Claim 6, the Examiner points to the teachings of Saville lines 1-5 as teaching this claimed feature. Applicants urge that Saville expressly teaches away from the features of Claim 6, as Saville describes a special command that can be used to launch an application at a different security level than the one that currently exists, in order to avoid a user having to logoff their current security context and re-login with a different security context. This special launching of an application, and as described at lines 4-5, is performed by a SU command. This SU command is a utility that allows a user to temporarily start applications running in the security context of a different account (Saville lines 4-5), and avoids the user from having to logoff (line 4). Thus, Saville expressly teaches away from the features of Claim 6, by teaching a technique that *avoids logoff*. In contrast, Claim 6 is explicitly directed to an action (reverting to the first security context) *in response to a user logoff*. Thus, it is urged that a proper prima facie case of obviousness has not been established by the Examiner as there are missing claimed features not taught or suggested by any of the cited references. Thus, Claim 6 is shown to have been erroneously rejected.

¹ In rejecting claims under 35 U.S.C. Section 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. *Id.* To establish prima facie obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. MPEP 2143.03. *See also, In re Royka*, 490 F.2d 580 (C.C.P.A. 1974). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

In conclusion, Appellants have shown error in the Examiner's final rejection of all claims, and thus requests that the Board reverse such final claim rejection of all claims.


Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
YEE & ASSOCIATES, P.C.
PO Box 802333
Dallas, TX 75380
(972) 385-8777

CLAIMS APPENDIX

The text of the claims involved in the appeal are:

1. An authentication method comprising the steps of:
generating a first security context in response to a first user authentication;
generating a second security context in response to a second user authentication, wherein
said second security context is an aggregate of said first security context and a security context
corresponding to an identity in said second user authentication.
2. The method of claim 1 further comprising the step of saving said first security context.
3. The method of claim 2 wherein said step of saving said first security context comprises
the step of pushing said first security context on a stack.
4. The method of claim 1 further comprising the step of receiving a user logoff.
5. The method of claim 4 further comprising the step of destroying said second security
context in response to said step of receiving said user logoff.
6. The method of claim 2 further comprising the step of reverting to said first security
context in response to a user logoff, wherein said first security context is then used to access
security protected resources by a user who issued the user logoff.

7. The method of claim 6 wherein said step of reverting to said first security context comprises the step of popping said first security context off of a stack.
8. The method of claim 1 further comprising the step of determining an access permission in response to said second security context.
9. A computer program product embodied in a tangible storage medium, the program product comprising a program of instructions for performing the method steps of:
 - generating a first security context in response to a first user authentication;
 - generating a second security context in response to a second user authentication, wherein said second security context is an aggregate of said first security context and a security context corresponding to an identity in said second user authentication.
10. The program product of claim 9 further comprising instructions for performing the step of saving said first security context.
11. The program product of claim 10 wherein said step of saving said first security context comprises the step of pushing said first security context on a stack.
12. The program product of claim 9 further comprising instructions for performing the step of receiving a user logoff.

13. The program product of claim 12 further comprising instructions for performing the step of destroying said second security context in response to said step of receiving said user logoff.

14. The program product of claim 10 further comprising instructions for performing the step of reverting to said first security context in response to a user logoff, wherein said first security context is then used to access security protected resources by a user who issued the user logoff.

15. The program product of claim 14 wherein said step of reverting to said first security context comprises the step of popping said first security context off of a stack.

16. The program product of claim 9 further comprising instructions for performing the step of determining an access permission in response to said second security context.

17. A data processing system comprising:

circuitry operable for generating a first security context in response to a first user authentication;

circuitry operable for generating a second security context in response to a second user authentication, wherein said second security context is an aggregate of said first security context and a security context corresponding to an identity in said second user authentication.

18. The system of claim 17 further comprising circuitry operable for saving said first security context.

19. The system of claim 18 wherein said circuitry operable for saving said first security context comprises the step of pushing said first security context on a stack.
20. The system of claim 17 further comprising circuitry operable for receiving a user logoff.
21. The system of claim 20 further comprising circuitry operable for destroying said second security context in response to said step of receiving said user logoff.
22. The system of claim 18 further comprising circuitry operable for reverting to said first security context in response to a user logoff, wherein said first security context is then used to access security protected resources by a user who issued the user logoff.
23. The system of claim 22 wherein said circuitry operable for reverting to said first security context comprises circuitry operable for popping said first security context off of a stack.
24. The system of claim 17 further comprising circuitry operable for determining an access permission in response to said second security context.

EVIDENCE APPENDIX

There is no evidence to be presented.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.